

Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore Maya (SBN 223242)
tmaya@ahdootwolfson.com
Bradley K. King (SBN 274399)
bking@ahdootwolfson.com
Christopher E. Stiner (SBN 276033)
cstiner@ahdootwolfson.com
Rachel Johnson (SBN 331351)
rjohnson@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 West Olive Ave., Suite 500
Burbank, CA 91505
Tel: (310) 474-9111
Fax: (310) 474-8585

Mark C. Molumphy (SBN 168009)
mmolumphy@cpmlegal.com
Joseph W. Cotchett (SBN 36324)
jcotchett@cpmlegal.com
Tyson Redenbarger (SBN 294424)
trredenbarger@cpmlegal.com
Noorjahan Rahman (SBN 330572)
nrahman@cpmlegal.com
Julia Peng (SBN 318396)
jpeng@cpmlegal.com
COTCHETT, PITRE & McCARTHY LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: 650.697.6000
Facsimile: 650.697.0577

Interim Co-Lead Class Counsel
Additional Counsel on Signature Page

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

IN RE: ZOOM VIDEO
COMMUNICATIONS, INC. PRIVACY
LITIGATION

This Document Relates To: All Actions

Case No. 5:20-CV-02155-LHK

**PLAINTIFFS' OPPOSITION TO
MOTION TO DISMISS**

Date: February 4, 2021
Time: 1:30 p.m.
Courtroom: 8, 4th Floor
Judge: Hon. Lucy H. Koh

TABLE OF CONTENTS

	Page
I. INTRODUCTION	- 1 -
II. BACKGROUND	- 1 -
III. ARGUMENT	- 2 -
A. Zoom Is Not Immune Under Section 230.....	- 3 -
1. Zoom is Not an Interactive Computer Service	- 3 -
2. Plaintiffs Do Not Seek to Treat Zoom as a Publisher or Speaker.....	- 4 -
B. Plaintiffs State a Claim for Invasion of Privacy	- 6 -
1. Plaintiffs Allege <i>Their</i> Data Was Shared.....	- 6 -
2. Plaintiffs Plead a Reasonable Expectation of Privacy	- 7 -
3. Plaintiffs Properly Plead the Intrusion Was Highly Offensive.....	- 10 -
C. Plaintiffs State a Claim for Negligence	- 11 -
1. The Economic Loss Doctrine is Inapplicable	- 11 -
2. Plaintiffs Properly Allege Violations of Duties Arising from Tort Law	- 11 -
3. Plaintiffs Had a Special Relationship with Zoom.....	- 12 -
4. Plaintiffs Sufficiently Plead the Elements of Negligence.....	- 14 -
D. Plaintiffs State a Claim for Breach of Implied Contract.....	- 16 -
E. Plaintiffs Allege Breach of the Covenant of Good Faith and Fair Dealing	- 18 -
F. Plaintiffs State Claims Under the UCL, CLRA, and for Fraudulent Concealment	- 20 -
1. Plaintiffs' Fraud-Based Claims Are Pled With Sufficient Particularity	- 20 -
2. Plaintiffs Sufficiently Allege Claims Based On Affirmative Statements.....	- 20 -
3. Plaintiffs Adequately Allege Reliance.....	- 21 -
4. Plaintiffs Adequately Allege Fraud-Based Claims	- 21 -
5. Plaintiffs State a CLRA Damages Claim.....	- 22 -
6. All Plaintiffs Suffered Economic Injury	- 22 -
7. Plaintiffs State Claims Under The UCL's Unlawful and Unfair Prongs.....	- 23 -
G. Plaintiffs State a Claim for Unjust Enrichment	- 24 -
H. Plaintiffs' CDAFA Claim Should Not Be Dismissed.....	- 24 -
IV. CONCLUSION	- 25 -

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Acri v. Varian Assocs., Inc.</i> , 121 F.3d 714 (9th Cir. 1997)	18
<i>In re Adobe Sys., Inc. Privacy Litig.</i> , 66 F. Supp. 3d 1197 (N.D. Cal. 2014)	21, 23
<i>In re Anthem, Inc. Data Breach Litig.</i> , 162 F. Supp. 3d 953 (N.D. Cal. 2016)	22, 23
<i>In re Apple & ATTM Antitrust Litig.</i> , No. C 07-05152, 2010 WL 3521965 (N.D. Cal. July 8, 2010).....	25
<i>Aron v. U-Haul Co.</i> , 143 Cal. App. 4th 796 (2006)	22
<i>Astiana v. Hain Celestial Grp., Inc.</i> , 783 F.3d 753 (9th Cir. 2015)	24
<i>Banga v. Equifax Information Services LLC</i> , 2015 WL 3799546 (N.D. Cal., 2015)	7
<i>Barnes v. Yahoo!, Inc.</i> , 570 F.3d 1096 (9th Cir. 2009)	3
<i>Be In, Inc. v. Google Inc.</i> , No. 12-cv-03373, 2013 WL 5568706 (N.D. Cal. Oct. 9, 2013)	17
<i>Brickman v. Fitbit, Inc.</i> , No. 15-cv-2077-JD, 2016 WL 3844327 (N.D. Cal. July 15, 2016).....	20
<i>Brodsky v. Apple Inc.</i> , No. 19-CV-00712, 2019 WL 4141936 (N.D. Cal. Aug. 30, 2019)	25
<i>Bruton v. Gerber Prods. Co.</i> , No. 12-CV-02412-LHK, 2018 U.S. Dist. LEXIS 149404 (N.D. Cal. Aug. 31, 2018).....	24
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	8, 11
<i>Castillo v. Seagate Tech., LLC</i> , No. 16-cv-01958-RS, 2016 WL 9280242 (N.D. Cal. Sept. 14, 2016).....	12, 16, 17
<i>Celador Int'l Ltd. v. Walt Disney Co.</i> , 347 F. Supp. 2d 846 (C.D. Cal. 2004)	19

1	<i>Clear Channel Outdoor, Inc. v. Bently Holdings Cal. L.P.</i> ,	
2	No. 11-2573 EMC, 2011 WL 6099394 (N.D. Cal. Dec. 7, 2011)	24
3	<i>Corona v. Sony Pictures Ent., Inc.</i> ,	
4	No. 14-cv-09600, 2015 WL 3916744 (C.D. Cal. June 15, 2015).....	13
5	<i>Davidson v. Apple, Inc.</i> ,	
6	No. 16-cv-4942-LHK, 2017 WL 976048 (N.D. Cal. Mar. 14, 2017).....	20, 21
7	<i>Davis v. Capitol Records, LLC</i> ,	
8	No. 12-CV-1602 YGR, 2013 WL 1701746 (N.D. Cal. Apr. 18, 2013).....	19
9	<i>Doe v. Internet Brands, Inc.</i> ,	
10	824 F.3d 846 (9th Cir. 2016)	14, 15
11	<i>Doe v. Kik Interactive, Inc.</i> ,	
12	No. 20-60702-CIV, 2020 WL 5156641 (S.D. Fla. Aug. 31, 2020)	4
13	<i>Doe v. MySpace</i> ,	
14	528 F.3d 413 (5th Cir. 2008)	5
15	<i>Dual Diagnosis Treatment Ctr., Inc. v. Blue Cross of Cal.</i> ,	
16	SA CV 15-0736, 2016 WL 6892140 (C.D. Cal. Nov. 22, 2016).....	18
17	<i>Dyroff v. Ultimate Software Grp., Inc.</i> ,	
18	934 F.3d 1093 (9th Cir. 2019)	4
19	<i>E&J Gallo Winery v. EnCana Energy Services, Inc.</i> ,	
20	2004 WL 7342782 (E.D.Cal., 2004).....	6
21	<i>In re Easysaver Rewards Litig.</i> ,	
22	737 F. Supp. 2d 1159 (S.D. Cal. 2010).....	19
23	<i>Ehret v. Uber Technologies, Inc.</i> ,	
24	68 F. Supp. 3d 1121 (N.D. Cal. 2014)	20
25	<i>Elias v. Hewlett-Packard Co.</i> ,	
26	903 F. Supp. 2d 843 (N.D. Cal. 2012)	22
27	<i>In re Experian Data Breach Litig.</i> ,	
28	No. SACV 15-1592, 2016 WL 7973595 (C.D. Cal. Dec. 29, 2016)	13
	<i>In re Facebook, Inc., Consumer Privacy User Profile Litig.</i> ,	
	402 F. Supp. 3d 767 (N.D. Cal. 2019)	14, 16
	<i>In re Facebook, Inc. Internet Tracking Litig.</i> ,	
	956 F.3d 589 (9th Cir. 2020)	<i>passim</i>
	<i>Fairfield v. Am. Photocopy Equip. Co.</i> ,	
	138 Cal. App. 2d 82 (1955)	12, 16

1	<i>FTC v. LeadClick Media, Ltd. Liab. Co.</i> ,	
	838 F.3d 158 (2d Cir. 2016).....	3
2	<i>Gitson v. Trader Joe's Co.</i> ,	
3	No. 13-cv-1333-WHO, 2014 WL 1048640 (N.D. Cal. Mar. 14, 2014)	21
4	<i>Gonzalez v. Google, Inc.</i> ,	
5	282 F. Supp. 3d 1150 (N.D. Cal. 2017)	4
6	<i>In re Google Android Consumer Privacy Litig.</i>	
	No. 11-MD-02264, 2013 WL 1283236, (N.D. Cal. Mar. 26, 2013).....	12
7	<i>In re Google Assistant Privacy Litig.</i> ,	
8	457 F. Supp. 3d 797 (N.D. Cal. 2020)	11, 23
9	<i>In re Google Inc. Cookie Placement Consumer Privacy Litig.</i> ,	
10	806 F.3d 125 (3d Cir. 2015).....	10
11	<i>Gordon v. Chipotle Mexican Grill, Inc.</i> ,	
	344 F. Supp. 3d 1231 (D. Colo. 2018).....	17
12	<i>Green v. Am. Online</i> ,	
13	318 F.3d 465 (3d Cir. 2003).....	5
14	<i>H&M Assocs. v. City of El Centro</i> ,	
15	109 Cal. App. 3d 399 (1980)	6
16	<i>Hameed-Bolden v. Forever 21 Retail, Inc.</i> ,	
	2018 WL 6802818 (C.D. Cal. Oct. 1, 2018).....	17
17	<i>Heeger v. Facebook, Inc.</i> ,	
18	No. 18-cv-06399-JD, 2019 WL 7282477 (N.D. Cal. Dec. 27, 2019).....	10
19	<i>Herrick v. Grindr, LLC</i> ,	
20	306 F. Supp. 3d 579 (S.D.N.Y. 2018).....	4
21	<i>Hickcox-Huffman v. US Airways, Inc.</i> ,	
	No. 10-cv-05193, 2017 WL 4842021 (N.D. Cal. Oct. 26, 2017)	17
22	<i>Hill v. NCAA</i> ,	
23	7 Cal. 4th 1 (1994)	7
24	<i>In re iPhone App. Litig.</i> ,	
25	844 F. Supp. 2d 1040 (N.D. Cal. 2012)	9
26	<i>J'Aire Corp. v. Gregory</i> ,	
	24 Cal. 3d 799 (1979)	12
27	<i>Jane Doe No. 1 v. Backpage.com, LLC</i> ,	
28	817 F.3d 12 (1st Cir. 2016).....	5

1	<i>Kalitta Air, L.L.C. v. Cent. Texas Airborne Sys., Inc.</i> ,	
2	315 F. App'x 603 (9th Cir. 2008)	11
3	<i>Kaufman & Broad Monterey Bay v. Travelers Prop. Cas. Co. of Am.</i> ,	
4	No. C10-02856 EJD, 2011 WL 2181692 (N.D. Cal. June 2, 2011)	6
5	<i>Kevin Barry Fine Art Assocs. v. Ken Gangbar Studio, Inc.</i> ,	
6	391 F. Supp. 3d 959 (N.D. Cal. 2019)	14
7	<i>Kwikset Corp. v. Super. Ct.</i> ,	
8	51 Cal. 4th 310 (2011)	22
9	<i>Low v. LinkedIn Corp.</i> ,	
10	900 F. Supp. 2d 1010 (N.D. Cal. 2012)	7, 9
11	<i>McDonald v. Kiloo ApS</i> ,	
12	385 F. Supp. 3d 1022 (N.D. Cal. 2019)	11
13	<i>Miller v. Nat'l Broad. Co.</i> ,	
14	187 Cal. App. 3d 1463 (1986)	12, 16
15	<i>Morgan v. AT & T Wireless Servs., Inc.</i> ,	
16	177 Cal. App. 4th 1235 (2009)	22
17	<i>N. Am. Chem. Co. v. Superior Court</i> ,	
18	59 Cal. App. 4th 764, 69 Cal. Rptr. 2d 466 (1997).....	16
19	<i>Nguyen v. Barnes & Noble Inc.</i> ,	
20	763 F.3d 1171 (9th Cir. 2014)	17
21	<i>Nunes v. Twitter, Inc.</i> ,	
22	194 F. Supp. 3d 959 (N.D. Cal. 2016)	5
23	<i>Organic Consumers Ass'n v. Sanderson Farms, Inc.</i> ,	
24	284 F. Supp. 3d 1005 (N.D. Cal. 2018)	16
25	<i>Oxina v. Lands' End, Inc.</i> ,	
26	No. 14-cv-2577-MMA, 2015 WL 4272058 (S.D. Cal. June 19, 2015)	22
27	<i>Patel v. Facebook, Inc.</i> ,	
28	932 F.3d 1264 (9th Cir. 2019)	8
	<i>Philips v. Ford Motor Co.</i> ,	
	No. 14-cv-2989-LHK, 2015 WL 4111448 (N.D. Cal. July 7, 2015).....	21
	<i>Pirozzi v. Apple Inc.</i> ,	
	913 F. Supp. 2d 840 (N.D. Cal. 2012)	21, 22
	<i>Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress</i> ,	
	402 F. Supp. 3d 615 (N.D. Cal. 2019)	16

1	<i>Pollstar v. Gigmania, Ltd.</i> ,	
2	170 F. Supp. 2d 974 (E.D. Cal. 2000).....	18
3	<i>In re Premera Blue Cross Customer Data Sec. Breach Litig.</i> ,	
4	No. 3:15-MD-2633-SI, 2017 WL 539578 (D. Or. Feb. 9, 2017).....	19
5	<i>Putensen v. Clay Adams, Inc.</i>	
6	12 Cal.App.3d 1062 (1970)	14, 15, 16
7	<i>R Power Biofuels, LLC v. Chemex LLC</i> ,	
8	No. 16-CV-00716-LHK, 2016 WL 6663002 (N.D. Cal. Nov. 11, 2016).....	11
9	<i>Randall v. Change.org, Inc.</i> ,	
10	2020 U.S. Dist. LEXIS 231632 (N.D. Cal. De. 9, 2020).....	17
11	<i>Riley v. California</i> ,	
12	573 U.S. 373 (2014).....	8
13	<i>Rudolph v. Hudson's Bay Co.</i> ,	
14	No. 18-CV-8472 (PKC), 2019 WL 2023713 (S.D.N.Y. May 7, 2019).....	17
15	<i>Sagana v. Tenorio</i> ,	
16	384 F.3d 731 (9th Cir. 2004)	23
17	<i>Scott-Codiga v. County of Monterey</i> ,	
18	No. 10-05450, 2011 WL 4434812 (N.D. Cal. 2011)	7
19	<i>Shin v. BMW of N. Am.</i> ,	
20	No. CV 09-398-AHM, 2009 WL 2163509 (C.D. Cal. July 16, 2009)	21
21	<i>Shultz v. TTAC Publ'g</i> ,	
22	LLC, 2020 U.S. Dist. LEXIS 198834 (N.D. Cal. Oct. 26, 2020)	18
23	<i>Sikhs for Justice "SFJ", Inc. v. Facebook, Inc.</i> ,	
24	144 F. Supp. 3d 1088 (N.D. Cal. 2015)	4
25	<i>In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.</i> ,	
26	No. 3:19-cv-2284-H-KSC, 2020 WL 2214152 (S.D. Cal. May 7, 2020).....	18, 19
27	<i>Swafford v. IBM</i> ,	
28	383 F. Supp. 3d 916 (N.D. Cal. 2019)	24
	<i>Tarasoff v. Regents of Univ. of California</i> ,	
	17 Cal. 3d 425 (1976)	15
	<i>Ticketmaster LLC v. Prestige Entm't W., Inc.</i> ,	
	315 F. Supp. 3d 1147 (C.D. Cal. 2018)	25
	<i>U.S. v. Jin</i> ,	
	No. 1:20-mj-01103-RER, Dkt. 1 (E.D.N.Y., unsealed Dec. 18, 2020)	2, 6

1	<i>United States v. Jones,</i>	
2	565 U.S. 400 (2012).....	8
3	<i>Vess v. Ciba-Geigy Corp. USA,</i>	
4	317 F.3d 1097 (9th Cir. 2003)	20
5	<i>In re Vizio Inc., Consumer Privacy Litig.,</i>	
6	238 F. Supp. 3d 1204 (C.D. Cal. 2017)	23
7	<i>In re Yahoo Mail Litigation</i>	
8	7 F. Supp. 3d 1016, 1039 (N.D. Cal. 2014)	11
9	<i>In re Yahoo! Inc. Customer Data Security Breach Litig.,</i>	
10	No. 16-MD-02752-LHK, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017).....	19
11	<i>In re Yahoo! Inc. Customer Data Security Breach Litigation,</i>	
12	313 F. Supp. 3d 1113 (N.D. Cal. 2018)	13
13	<i>Zbitnoff v. Nationstar Mortgage, LLC,</i>	
14	2014 WL 1101161 (N.D. Cal., 2014)	7
15	Statutes	
16	47 U.S.C § 230(c)(1).....	3, 4, 5
17	Cal. Civ. Code § 43.92.....	15
18	Cal. Penal Code § 502(c)(1), (2), (3), and (7).....	25
19	Other Authorities	
20	Fed. R. Civ. Proc.	
21	Rule 9(b)	20, 21
22	Rule 15	25

I. INTRODUCTION

Zoom’s ultra-lax security and privacy practices resulted in subpar, poorly secured meetings, disclosure of Plaintiffs’ and other class members’ personal information, including detailed device information and unique identifiers (collectively, “PII”), and offensive and harmful meeting intrusions.

Contrary to Zoom’s assertions, Plaintiffs fully allege that Zoom disclosed *their* PII to third parties, and failed to secure meetings with adequate security protocols and encryption as promised. Plaintiffs further fully allege that they only used Zoom in reliance on Zoom’s false promises that it took privacy and security seriously, and that it would protect their personal information. Each of Plaintiffs’ claims for these privacy violations is well-pled, and Zoom’s motion to dismiss (Dkt. 134 (“Mot.”)) should be denied.

II. BACKGROUND

Zoom provides a video conferencing service that users can access via computer, tablet, smartphone, or traditional telephone. ¶¶69-70.¹ In early 2020, usage of Zoom video services increased dramatically in response to the COVID-19 pandemic, reaching more than 200 million daily users. ¶4. Plaintiffs are individuals and entities harmed by Zoom’s misrepresentations and security failures.

First, Plaintiffs were harmed when Zoom shared their PII with third-parties without permission, including for example with Facebook, Google, and subscribers to LinkedIn’s sales prospecting application. ¶¶5, 8, 14. The PII Zoom admits it shared with Facebook includes device carrier, iOS Advertiser ID, iOS Device CPU Cores, iOS Device Display Dimension, iOS Device Model, iOS Language, iOS Time zone, iOS Version, even if the user did not have a Facebook account. ¶¶5, 13, 78. Zoom’s admission in this regard is incomplete, and Plaintiffs allege further details, including that the PII included device data allowing Facebook to conduct near-perfect, detailed surveillance of individual lives by learning, for example, a user’s entire Zoom activity including the nature of meetings. ¶¶94-99.

Zoom shares similarly valuable user data with Google via Google’s Firebase Analytics tracker, including GPS location data. ¶¶106-10. Zoom also revealed the identity of meeting participants, along with their personal information, to subscribers of its LinkedIn sales prospecting application, even when participants took steps to ensure their anonymity. ¶¶122-27. “Zoom’s data sharing is not limited to

¹ “¶” cites refer to paragraphs in Plaintiffs’ First Amended Consolidated Class Action Complaint (Dkt. 126 (“FAC”)).

1 Facebook, Google, and LinkedIn. Zoom also sends personal data about [its] users to hotjar, Zendesk,
2 AdRoll, Bing, and others.” ¶128.

3 Second, Zoom misstated the security capabilities and offerings of its services where Zoom failed
4 to provide end-to-end encryption (“E2EE”), as promised. ¶¶7, 163-66. Zoom’s service is not E2EE, and
5 Zoom itself has access to the video and audio of all Zoom meetings. ¶168. Plaintiffs relied on these
6 misrepresentations, including the green lock Zoom displayed in the top left corner of the application,
7 which stated “Zoom is using an end to end encrypted connection.” ¶¶19, 166. Not only are Zoom
8 meetings not E2EE, but they may also be recorded and/or automatically transcribed. ¶¶151-52.
9 Additionally, before April 2020, Zoom included a surreptitious “attention tracker feature” that “gave
10 presenters the ability to ‘track if participants . . . clicked away from the active Zoom window for more
11 than half a minute.’” ¶150 (citations omitted).

12 Third, Zoombombing (which continues today) has harmed Plaintiffs and the Class. Zoombombing
13 involves security breaches during which unauthorized intruders hijack Zoom meetings, display
14 pornography and graphic violence, shout racial epitaphs, or engage in comparably highly offensive,
15 despicable conduct. ¶9. Plaintiffs and the Class have suffered real harm as a result of Zoombombing,
16 including severe emotional trauma that required, for example, Plaintiff Oak Life Church to hire trauma
17 counselors. ¶41. Since the FAC was filed, Plaintiffs learned that, in some cases, Zoom’s own employees
18 engaged in Zoombombing in order to fabricate excuses to terminate those meetings at the request of the
19 Chinese government. *See U.S. v. Jin*, No. 1:20-mj-01103-RER, Dkt. 1 (E.D.N.Y., unsealed Dec. 18, 2020)
20 at ¶¶ 55-56, 79-81.

21 At the motion to dismiss stage, all of Plaintiffs’ “allegations of material fact are taken as true and
22 construed in the light most favorable” to them as the non-moving party. *In re Facebook, Inc. Internet*
23 *Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (hereinafter “*Facebook Internet Tracking*”).

24 **III. ARGUMENT**

25 Contrary to Defendant’s arguments (*e.g.*, Mot. at 8-9, 11), Plaintiffs adequately allege that *their*
26 data was disclosed. Specifically, Plaintiffs allege that the dissemination of users’ PII through the
27 Facebook SDK *occurs automatically* and, thus, impacted *all* users utilizing Zoom’s app. *See, e.g.*, ¶85
28 (“From the very first install and launch of an app (such as Zoom) that utilizes Facebook’s SDK, data is

sent to Facebook.”); ¶¶99 (“Even for individuals without a Facebook account, a shadow profile is built based on a compilation of app usage on the specific individuals’ device.”). Via similar means, Plaintiffs allege that Zoom also shares *their* PII with Google, including precise location information. ¶¶106-10.

Plaintiffs more than adequately allege personal harm as to each cause of action by, among other things, alleging loss of money or other valuable consideration, including on behalf of those Plaintiffs (Hartmann, Simins, Gormezano, Hirschberg, Garcia, Doyle, Saint Paulus, and Oak Life) who purchased paid accounts (¶¶17, 36, 39, 43, 50, 53, 56, 58, 221, 225, 235-37, 245, 261); loss of benefit of the bargain (¶¶146, 235-36); loss of clientele (¶45); other out-of-pocket expenses including Oak Life Church’s need to hire trauma counselors (¶41); violation of Plaintiffs’ right to privacy through unauthorized data collection and dissemination (¶¶5, 78, 106-10, 124-27); diminished value of PII (¶¶6, 148, 221, 261); and emotional distress (¶¶37, 41, 179, 221).

A. Zoom Is Not Immune Under Section 230

Zoom argues that the Communications Decency Act, 47 U.S.C. § 230 (“Section 230”) immunizes it from liability here. Mot. at 4.² However, Section 230 only protects “(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider.” *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100–01 (9th Cir. 2009). Section 230 does not apply because Zoom is not an interactive computer service and Plaintiffs do not treat it as a publisher or speaker.

1. Zoom is Not an Interactive Computer Service

“[I]nternet service providers, website exchange systems, online message boards, and search engines fall within this definition.” *FTC v. LeadClick Media, Ltd. Liab. Co.*, 838 F.3d 158, 174 (2d Cir. 2016). These services are typically *public* advertisement websites, *public* internet message boards, or *public* search engines. *Id.* “The prototypical service qualifying for [CDA] immunity is an online messaging board (or bulletin board) on which Internet subscribers post comments and respond to

² Zoom does not argue Section 230 provides *carte blanche* immunity for privacy claims. Additionally, Zoom is wrong to suggest that Plaintiffs’ invasion of privacy and negligence claims are premised solely on Zoombombing (Mot. at 4 n.4), as those claims clearly are premised on Zoom’s violations of Plaintiffs’ privacy rights, including its unauthorized sharing of their PII with third parties.

1 comments posted by others.” *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1097 (9th Cir. 2019).

2 Zoom is not an interactive computer service. Unlike a platform intended for users to publicly
3 share, exchange, and *post* content to a specific website (e.g., YouTube, Facebook, LinkedIn), Zoom
4 provides video and audio *conferencing* services. ¶¶3, 12, 64. Zoom does not publish its users’ calls and
5 there are no public comments. ¶¶65-72. Rather, Zoom calls are intended to involve only the invited
6 participants for a finite duration. Thus, Zoom is more akin to a modern-day telephone utility, facilitating
7 telephone and video calls over the internet—and users frequently join Zoom calls by dialing in from their
8 telephones (landlines included), without using a computer. ¶¶70-71.

9 Granting Zoom’s request to treat it like the video version of an online message board (Mot. at 5-
10 6), would be inconsistent with the services Zoom provides and Congress’s intent in providing immunity
11 for websites that publish information. *See Gonzalez v. Google, Inc.*, 282 F. Supp. 3d 1150, 1157 (N.D.
12 Cal. 2017) (“[Section 230] protects websites from liability for material posted on the website by someone
13 else.”). Accordingly, Zoom’s cited cases are distinguishable as they involve search engines, social media
14 networks, or public platforms for users to browse and respond to posted content. In fact, *Herrick* reaffirms
15 that interactive computer services under Section 230 are “networking sites like Facebook.com[] and online
16 matching services like Roommates.com[, . . .] Matchmaker.com,” and Grindr. *Herrick v. Grindr, LLC*,
17 306 F. Supp. 3d 579, 588 (S.D.N.Y. 2018); *see also Doe v. Kik Interactive, Inc.*, No. 20-60702-CIV, 2020
18 WL 5156641, at *1 (S.D. Fla. Aug. 31, 2020) (interactive social media service falls within Section 230).
19 Zoom’s final assertion that it qualifies as an interactive computer service simply because it has “hundreds
20 of millions of users” is unsupported. Mot. at 5. The number of users is irrelevant under Section 230.

21 **2. Plaintiffs Do Not Seek to Treat Zoom as a Publisher or Speaker**

22 Even if Zoom were an interactive computer service (it is not), Section 230 immunity would not
23 apply because Plaintiffs do not seek to treat Zoom as “the publisher or speaker of any information provided
24 by another information content provider.” 47 U.S.C § 230(c)(1). “[P]ublication involves reviewing,
25 editing, and deciding whether to publish or to withdraw from publication third-party content.” *Sikhs for*
26 *Justice “SFJ”, Inc. v. Facebook, Inc.*, 144 F. Supp. 3d 1088, 1094 (N.D. Cal. 2015).

27 Plaintiffs seek to hold Zoom accountable for its failure to provide promised security and privacy
28 during Zoom calls, not for Zoom’s actions as a content provider, publisher, or speaker. ¶¶177, 180-182.

Zoom’s liability does not depend on any assertion that it is required to sift through content to make sure the content is not offensive. Instead, Plaintiffs seek to hold Zoom liable for its failure to provide security and safeguards to prevent meeting intrusions, regardless of the specific content of such intrusions. *See Nunes v. Twitter, Inc.*, 194 F. Supp. 3d 959, 967-68 (N.D. Cal. 2016); *see also* ¶¶177, 180-182. Accordingly, Section 230 immunity does not apply in this case.

Zoom’s cases are inapplicable. In *Doe v. MySpace*, 528 F.3d 413 (5th Cir. 2008), the plaintiff and an assailant each created public MySpace profiles and voluntarily communicated online and offline; there was no Zoombombing-like conduct; rather, the plaintiff alleged MySpace should have excluded *the plaintiff*, who lied about her age, from using the social network, not the assailant. *Id.* at 420. Here, Plaintiffs allege that Zoom, a video conferencing services provider, negligently failed to provide secure conferencing services. Plaintiffs do not seek to hold Zoom liable as a publisher or speaker.

The remainder of cases Zoom cites discuss Section 230 in the context of publicly posted information on *websites*. This case is unlike *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12 (1st Cir. 2016) and the cases cited therein, where the claims involved *public postings* on message boards, social media websites, online classified forums, and online dating sites. Mot. at 18-19. Zoom simply does not provide an online platform where users publish information. Zoom users do not post advertisements, videos, or any content to Zoom’s website. Accordingly, *Green v. Am. Online*, 318 F.3d 465, 472 (3d Cir. 2003) is inapplicable as it concerned derogatory comments posted in a *public* chat room. Plaintiffs here do not seek to hold Zoom liable for developing unwanted content or for failing to *ensor* video conference calls. Rather, Plaintiffs’ seek to hold Zoom responsible for failing to provide privacy and security that would prevent unwanted intrusions into their private gatherings.

Zoom’s claim that there is no evidence of third party hacking or unauthorized access is unsupported in light of recently unveiled evidence to the contrary. On December 18, 2020, the Department of Justice’ U.S. Attorney’s Office for the Eastern District of New York (EDNY) (“DOJ”) unsealed a criminal complaint against a Zoom employee for, among other things, conspiring with the Chinese government to terminate meetings among political dissidents. The defendant is specifically accused of invading Zoom meetings and accessing Zoom customer accounts. The unauthorized access to meetings and accounts was possible because Zoom employees transmitted account credentials for US-based users,

allowing other Zoom employees to “Zoombomb” meetings in order to fabricate reports of Terms of Service violations. *See U.S. v. Jin*, No. 1:20-mj-01103-RER, Dkt. 1 (E.D.N.Y. filed Nov. 18, 2020, unsealed Dec. 18, 2020) at ¶¶ 55-56, 79-81. The DOJ complaint, therefore, directly contradicts Zoom’s claim that it plays no role whatsoever in Zoombombing.

B. Plaintiffs State a Claim for Invasion of Privacy³

1. Plaintiffs Allege *Their* Data Was Shared

Plaintiffs allege Zoom disclosed the personal information of users—including Plaintiffs—to third-parties, with great specificity. The FAC details specific information that Zoom’s CEO admitted was transmitted to Facebook including “device carrier, iOS Advertiser ID, iOS Device CPU Cores, iOS Device Display Dimension, iOS Device Model, iOS Language, iOS Time zone, iOS Version.” ¶78. These were only “examples” of information shared, implying the list was incomplete. ¶¶78-80. Data collection by third party trackers, like the Facebook SDK, does not vary among users. Data is sent to Facebook from *everyone* who uses Zoom’s application integrating the SDK. ¶85. Plaintiffs identify additional categories of data shared with Google and others and explain its value at length. ¶¶108, 111-21, 128. Plaintiffs allege this information allows Facebook, Google, and others to continuously surveil their daily lives on a granular level and track their physical location. ¶86.

More specifics are not required, particularly where Zoom is the only one with full knowledge of the full extent of its improper disclosures. *See E&J Gallo Winery v. EnCana Energy Services, Inc.*, 2004 WL 7342782, at *5 (E.D.Cal., 2004) (“The leeway typically granted a pleader is greater where the opposing party has exclusive control over information.”).

Zoom argues that its admission of sharing similarly situated users’ data with Facebook is inadequate to allege Plaintiffs’ PII was released to third parties, but Zoom provides no case law to support that position. The claims in the cases cited by Zoom were dismissed because the *specific type* of

³ As an initial matter Zoom argues that two institutional plaintiffs—St. Paulus and Oak Life—cannot maintain actions for invasion of privacy. But in California, “regardless of their legal form, [such entities] have zones of privacy which may not be legitimately invaded.” *H&M Assocs. v. City of El Centro*, 109 Cal. App. 3d 399, 410 (1980); *Kaufman & Broad Monterey Bay v. Travelers Prop. Cas. Co. of Am.*, No. C10-02856 EJD, 2011 WL 2181692, at *4 (N.D. Cal. June 2, 2011) (finding private right of action for invasion of privacy for a corporation turns on the nature of the information allegedly disclosed rather than an absolute bar). Thus, this analysis and response applies for all Plaintiffs.

1 information disclosed was *not specified*, not because the plaintiffs alleged they were members of a class
2 whose specifically-described information was released.⁴ Plaintiffs’ allegations here are sufficient.

3 **2. Plaintiffs Plead a Reasonable Expectation of Privacy**

4 As the Ninth Circuit recently framed the elements of Plaintiffs’ claims while reversing dismissal
5 under analogous circumstances, Plaintiffs must allege “(1) there exists a reasonable expectation of privacy,
6 and (2) the intrusion was highly offensive.” *Facebook Internet Tracking*, 956 F.3d F.3d at 601 (citing
7 *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009)). Both of these issues present “mixed questions
8 of law and fact.” *Hill v. NCAA*, 7 Cal. 4th 1, 40 (1994).

9 Plaintiffs expected that when Zoom specifically represented its service as safe and secure—and
10 that it was not sharing information with third parties—Zoom would not surreptitiously send users’ PII to
11 third parties. Zoom argues the data it shared without consent was merely “technical device data or publicly
12 available information” (Mot. at 12) but, to the contrary, the FAC specifically alleges it is precisely these
13 ostensibly benign categories of data, surreptitiously collected from users’ devices (¶78), that are the very
14 means used to continuously surveil devices. Recipients of this data (like Google and Facebook) use this
15 surveillance of a user’s device to develop highly detailed profiles on users, “ultimately identifying
16 characteristics such as race, age, sexual orientation, relationship status, socioeconomic status, parental
17 status.” ¶88. Similarly, the vast majority of Zoom users, like Plaintiffs, are unaware of Zoom’s extensive
18 ecosystem of apps such as the LinkedIn Sales Navigator App. Users had no reason to anticipate that Zoom
19 would take their LinkedIn profile data and connect it to their Zoom account without notifying them or
20 asking permission. Zoom did not require users in the meeting to *also* subscribe to LinkedIn’s service for
21 the video conferencing platform to access it.

22 Zoom argues Plaintiffs did not allege explicitly that they “sought anonymity.” Mot. at 12. But it

23 _____
24 ⁴ See *Scott-Codiga v. County of Monterey*, No. 10-05450, 2011 WL 4434812, at *6 (N.D. Cal. 2011)
25 (allegations of disclosed emails without further specifics deemed insufficient); *Zbitnoff v. Nationstar*
26 *Mortgage, LLC*, 2014 WL 1101161, at *4 (N.D. Cal., 2014) (“Plaintiff does not identify exactly what
27 private information defendants are alleged to have disclosed.”); *Banga v. Equifax Information Services*
28 *LLC*, 2015 WL 3799546, at *9 (N.D. Cal., 2015) (“Banga . . . does not explain what particular
information was disclosed or why that information qualifies as offensive and objectionable.”); *Low v.*
LinkedIn Corp., 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (“Although Plaintiffs postulate that these
third parties could, through inferences, de-anonymize this data, it is not clear that anyone has actually
done so, or what information, precisely, these third parties have obtained.”).

1 is not necessary to seek complete anonymity to establish an expectation of privacy, particularly where, as
 2 alleged, Zoom meetings “have replaced conference rooms, churches and temples, AA meeting rooms,
 3 schools, and healthcare professionals’ offices.” ¶12. No reasonable person would expect his or her PII,
 4 including detailed location information, work history, job titles, and more, to be disclosed during a
 5 conference call simply by joining it, especially when Zoom promises user privacy. Moreover, these are
 6 mixed questions of law and fact and Plaintiffs’ sufficiently allege an expectation of privacy.

7 There is a common societal understanding that ordinary people can conduct their daily affairs
 8 without records being surreptitiously kept of their movements. “[I]ndividuals maintain the expectation
 9 that entities will not be able to collect . . . broad swaths of personal information absent consent.” *Facebook*
 10 *Internet Tracking*, 956 F.3d at 604 n.7; *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (holding that
 11 individuals have a reasonable expectation of privacy in long-term location tracking); *Riley v. California*,
 12 573 U.S. 373, 397-99 (2014) (holding that individuals have a reasonable expectation of privacy in the
 13 contents of their cell phones). Zoom claimed to honor those expectations in its public statements. *See*,
 14 e.g., ¶¶75, 139, 143. Plaintiffs, therefore, had a reasonable expectation of privacy in the information Zoom
 15 shared without their permission and in violation of its public representations regarding privacy.

16 In *Carpenter*, the Supreme Court specifically held “that an individual maintains a legitimate
 17 expectation of privacy in the record of his physical movements as captured through [cell phone call
 18 records].” 138 S.Ct. at 2217; *see also United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J.,
 19 concurring) (finding that long term monitoring of location data via GPS technology “impinges on
 20 expectations of privacy”). The Court explained that the “unique nature of cell phone location information”
 21 presents a “new phenomenon: the ability to chronicle a person’s past movements.” *Carpenter*, 138 S. Ct.
 22 at 2216, 2220. The Ninth Circuit observes that such “[t]echnological advances provide ‘access to a
 23 category of information otherwise unknowable,’ and ‘implicate privacy concerns’” in new and different
 24 ways than before the age of big data. *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting
 25 *Riley*, 573 U.S. at 393). The threat posed by the storage of personal data over time—both as to tracking
 26 individually sensitive locations *and* as to divining “otherwise unknowable” inferences from the sum of
 27 stored information, which impelled the *Carpenter* Court to conclude citizens have a reasonable
 28 expectation of privacy in the geolocation records maintained by telecommunications providers, is

1 analogous to Zoom’s disclosures to Facebook and Google here.

2 In *Facebook Internet Tracking*, Facebook argued, much as Zoom does now, that plaintiffs had “to
3 identify specific, sensitive information that Facebook collected” to allege any concrete privacy interest.
4 956 F.3d at 603; Mot. at 10. The Ninth Circuit disagreed: “The question is not necessarily whether
5 Plaintiffs maintained a reasonable expectation of privacy in the information in and of itself,” but “whether
6 the data itself is sensitive *and* whether the manner it was collected—after users had logged out—violates
7 social norms.” 956 F.3d at 603 (emphasis in original). Here, Plaintiffs similarly allege Zoom provides
8 information necessary to continuously track Plaintiffs movements and device activity, even when they are
9 not using Zoom’s services, and even when they do not even have a Facebook account. ¶¶61-62, 104.

10 “[I]t is important to recognize that in the [last] six to eight years . . . , much has been learned about
11 the ability of technology giants ‘to amass a great degree of personalized information.’” *Facebook Internet*
12 *Tracking*, 956 F.3d at 599. On this basis, the Ninth Circuit critiqued much of Zoom’s cited authority,
13 reasoning that plaintiffs in *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012), and *In re*
14 *iPhone App. Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012), did not allege tracking outside of active use
15 of the defendants’ services. *Facebook Internet Tracking*, 956 F.3d at 606 n.8. In *Low*, Plaintiffs allege
16 that Defendant disclosed to third parties the LinkedIn ID and the URL of the LinkedIn profile page that
17 the user viewed (which in the aggregate discloses a user’s browsing history among LinkedIn
18 profiles). *Low*, 900 F. Supp. 2d at 1025. This case also is distinguishable in that Plaintiffs here identify
19 “what information, precisely, these third parties have obtained.” *Id.* Perhaps most importantly, it is more
20 clear today than in 2012 when *Low* and *In re iPhone App* were decided, that the sort of information Zoom
21 shares with third parties is shared for the sole purpose of near-perfect surveillance of those to whom it
22 pertains. Indeed, the purpose of the fingerprinting alleged is to determine the precise behaviors and
23 movements of users to precisely target advertising. ¶¶ 88-105. Furthermore, the amount of data required
24 to create a detailed map of one’s life is counterintuitively low—even with a small trove of “anonymized”
25 location data, *New York Times* reporters were able to tie cell phone “pings” included in that data to
26 individuals with ease, generating maps of, essentially, those individuals’ entire daily lives.⁵

27 ⁵ Charlie Warzel and Stuart A. Thompson, *Where Even the Children Are Being Tracked*, NEW YORK
28 TIMES (December 21, 2019).

3. Plaintiffs Properly Plead the Intrusion Was Highly Offensive

Plaintiffs also satisfy the second prong of the two-part test for pleading invasion of privacy under the California Constitution and common law. *See Facebook Internet Tracking*, 956 F.3d at 601. Plaintiffs’ allegations that Zoom’s conduct is highly offensive are supported with some fifteen pages of material facts detailing Zoom’s data sharing and how third parties aggregate that data through device “fingerprinting” and location tracking. ¶¶73, 78-80, 88-89, 98-105, 111-112, 124-128. Fingerprinting and tracking using the data identified by Plaintiffs are specifically intended to circumvent user choice and eliminate the ability to erase one’s digital identity. ¶101. Even Google engineers have opined such fingerprinting “subverts user choice and is wrong.” ¶105.

Zoom argues that this conduct is not highly offensive (or an “egregious breach of social norms”), yet none of Zoom’s authorities address any conduct as offensive as the location tracking via mobile devices or fingerprinting that Plaintiffs allege. Mot. at 12-13. *Facebook Internet Tracking* is more on point where the Ninth Circuit recognized that offensiveness is a question of fact that should be resolved on a full record. *Facebook Internet Tracking*, 956 F.3d at 606 (“The ultimate question of whether Facebook’s tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage.”). Further, Zoom concealed its insufficient security practices and data sharing. ¶¶129-48. “[D]eceit can be a ‘kind of “plus” factor [that is] significant in establishing an expectation of privacy or making a privacy intrusion especially offensive.” *Heeger v. Facebook, Inc.*, No. 18-cv-06399-JD, 2019 WL 7282477, *4 (N.D. Cal. Dec. 27, 2019) (quoting *McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1036 (N.D. Cal. 2019)); *see also In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 150-51 (3d Cir. 2015) (reasoning “deceit and disregard” were relevant to holding that California constitutional and privacy tort claims were well-pled).

Consistent with the Supreme Court’s recognition that the collection of mobile device location data implicates constitutional privacy interests, courts in this district have held that even apparently routine data collection practices may be highly offensive, especially when conducted secretly or deceptively. For example, Judge Donato denied a motion to dismiss where, as here, plaintiffs alleged the unauthorized collection of user data sufficient to generate unique profiles of individuals. “Current privacy expectations are developing” with respect to “whether a commercial entity that secretly harvests [such PII] commits a

highly offensive or egregious act.” *McDonald*, 385 F. Supp. 3d at 1035. The court could not “say that the answers are so patently obvious that the plaintiffs’ allegations are implausible or inadequate.” *Id.*

In re Yahoo Mail Litigation fails to support Zoom’s position, given that plaintiffs there failed to allege “facts regarding the content of their emails, their intent in sending those emails, the circumstances under which those emails were sent, or who the recipients of those emails were.” 7 F. Supp. 3d 1016, 1039 (N.D. Cal. 2014). The question was whether the emails themselves were sensitive. Similarly, in *Google Assistant Privacy Litig*, No. 19-cv-04286-BLF, ---F. Supp. 3d---, 2020 WL 2219022, at *19 (N.D. Cal. May 6, 2020), “Plaintiffs ha[d] not alleged sufficient information about the conversations that were allegedly intercepted and recorded.”

Here, by contrast, Plaintiffs allege many specifics concerning the PII that Zoom shared with Facebook, Google, and others, without Plaintiffs’ consent and in violation of its own privacy policy. Accordingly, the relevant authority is *Carpenter* and *Facebook Internet Tracking*. *Carpenter* recognized, when collected over time, stored information like that which Plaintiffs allege Zoom shared with Facebook, Google, and others (¶¶78-80, 86, 105, 108, 111-121, 128) “provides an intimate window into a person’s life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations.” 138 S. Ct. at 2217.

C. Plaintiffs State a Claim for Negligence

1. The Economic Loss Doctrine is Inapplicable

Zoom’s invocation of the economic loss rule (Mot. at 14-15) is misplaced. The economic loss rule does not apply if “(1) a ‘special relationship’ exists between the plaintiff and the defendant, . . . (2) the conduct ‘violates a duty independent of the contract arising from principles of tort law,’” or (3) the case involves personal injury. See *R Power Biofuels, LLC v. Chemex LLC*, No. 16-CV-00716-LHK, 2016 WL 6663002, at *4 (N.D. Cal. Nov. 11, 2016) (citations omitted); *Kalitta Air, L.L.C. v. Cent. Texas Airborne Sys., Inc.*, 315 F. App’x 603, 605 (9th Cir. 2008). Here, Plaintiffs allege all three: (1) violations of several duties independent of any contract arising from principles of tort law, (2) a special relationship between Plaintiffs and Zoom, and (3) personal injury.

2. Plaintiffs Properly Allege Violations of Duties Arising from Tort Law

Plaintiffs allege, *inter alia*, tort damages for invasion of privacy caused by Zoom’s negligence.

1 The right to privacy that Zoom violated is a right independent of any contractual duty. *See Facebook*
 2 *Internet Tracking*, 956 F.3d at 601 (describing California privacy tort law); *Miller v. Nat'l Broad. Co.*, 187
 3 Cal. App. 3d 1463, 1481-82 (1986) (“The right of privacy has been described as ‘independent of the
 4 common rights of property, contract, reputation and physical integrity.’”) (quoting *Gill v. Curtis Pub. Co.*,
 5 38 Cal. 2d 273, 276 (1952)); *Fairfield v. Am. Photocopy Equip. Co.*, 138 Cal. App. 2d 82, 87–88 (1955)
 6 (“The right is distinct in and of itself and not merely incidental to some other recognized right for breach
 7 of which an action for damages will lie. Violation of the right is a tort.”). Furthermore, damages are
 8 available notwithstanding any contractual or economic damages. *Facebook Internet Tracking*, 956 F.3d
 9 at 601 (describing right to “disgorgement of unjustly earned profits” earned through violations of users’
 10 privacy rights under California law); *Miller*, 187 Cal. App. 3d at 1485 (“One whose right of privacy is
 11 unlawfully invaded is entitled to recover substantial damages, although the only damages suffered by him
 12 resulted from mental anguish.”) (citing *Fairfield*, 138 Cal. App. 2d at 89). Plaintiffs also allege mental
 13 suffering (*i.e.*, personal injury) from Zoom’s failure to preclude Zoombombers. ¶¶37, 41.

14 The cases cited by Zoom, concerning losses related to monitoring fraudulent activity, are
 15 inapplicable. Mot. at 14. *Castillo v. Seagate Tech., LLC*, did not involve a claim for invasion of privacy,
 16 nor did it involve claims of emotional distress. *See* No. 16-CV-01958, 2016 WL 9280242, at *2, 4 (N.D.
 17 Cal. Sept. 14, 2016). Likewise, *In re Google Android Consumer Privacy Litig.* did not involve a claim
 18 for emotional distress. *See* No. 11-MD-02264, 2013 WL 1283236, at *12 (N.D. Cal. Mar. 26, 2013).

19 **3. Plaintiffs Had a Special Relationship with Zoom**

20 Plaintiffs also adequately alleged facts establishing that a “special relationship” exists, making the
 21 economic loss rule inapplicable. “What we mean by special relationship is that the plaintiff was an
 22 intended beneficiary of a particular transaction but was harmed by the defendant’s negligence in carrying
 23 it out.” *So. Cal. Gas Leak Cases*, 7 Cal. 5th 391, 400 (2019). Courts look to a number of factors in
 24 determining whether a special relationship exists:

25 (1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of
 26 harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness
 27 of the connection between the defendant's conduct and the injury suffered, (5) the moral blame
 attached to the defendant's conduct and (6) the policy of preventing future harm.

28 *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979); *see also So. Cal. Gas Leak Cases*, 7 Cal. 5th at 401

(similar factors).⁶

First, Zoom promoted its services as a virtual platform for Plaintiffs’ regular in-person activities. As such, Plaintiffs used Zoom’s services to hold bible studies (§33), prayer meetings and church services (§39), meetings with psychologists (§23), burlesque dance classes (§45), speech therapy meetings with students (§48), and meetings with patients (§52)—each with the understanding that Zoom would adequately protect Plaintiffs’ privacy and inform Plaintiffs of breaches or risks. §§12, 18, 19, 22, 25, 30, 34, 35, 40, 44, 47, 51. This is sufficient to establish the first factor. *See Yahoo! II*, 313 F. Supp. 3d at 1132 (holding economic loss rule inapplicable in data breach case).

Second, it was plainly foreseeable that Plaintiffs would suffer harm if Zoom did not adequately secure the service, protect the privacy of its users, or warn of known offenders. *See e.g.*, §§37, 41, 66-70, 78-80, 143-148. **Third**, the FAC leaves no doubt that Plaintiffs suffered harm—for example, Plaintiffs allege hackers were able to gain access to video calls, that church groups were shown pornography (§37, 41) and that dance classes were disrupted and clients were lost (§45). Additionally, Zoom negligently transferred Plaintiffs’ personal data to third parties without notice or permission. §5. **Fourth**, the injury was allegedly suffered exactly because Zoom “provided inadequate security and knew that [its] system was insufficient.” *Yahoo! II*, 313 F. Supp. 3d at 1132; *see also* §§38, 42. **Fifth**, it is appropriate to blame Zoom because it subordinated security and privacy in favor of grabbing market share despite knowing of significant security problems with its service. Zoom did nothing to prevent or warn Plaintiffs before it was too late. *Id.*; *See Yahoo! II*, 313 F. Supp. 3d at 1132 (“Defendants are morally culpable, given their repeated security breaches, wholly inadequate safeguards, and refusal to notify Plaintiffs...of breaches or security vulnerabilities.”). **Sixth**, public policy supports protecting privacy and consumer data, as evidenced by the concerns expressed in state and federal privacy statutes. “‘In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively.’ For this reason, our country has countless federal laws on the books designed to protect our privacy – laws

⁶ Courts generally do not apply the economic loss rule to bar privacy claims. *See, e.g., In re Yahoo! Inc. Customer Data Security Breach Litigation* (hereinafter, “*Yahoo! II*”), 313 F. Supp. 3d 1113, 1131 (N.D. Cal. 2018); *In re Experian Data Breach Litig.*, No. SACV 15-1592, 2016 WL 7973595 (C.D. Cal. Dec. 29, 2016); *Corona v. Sony Pictures Ent., Inc.*, No. 14-cv-09600, 2015 WL 3916744 (C.D. Cal. June 15, 2015).

that the federal courts are charged with enforcing.” *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 776, 786 (N.D. Cal. 2019) (internal citations omitted) (quoting *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001)). Accordingly, Plaintiffs have adequately pled a “special relationship,” thus Plaintiffs’ negligence claims are not barred by the economic-loss rule.

4. Plaintiffs Sufficiently Plead the Elements of Negligence

a. Zoom Breached Its Duty to Prevent Third Party Access⁷

Plaintiffs sufficiently allege that Zoom breached its duty to protect their users’ personal information. As described in the FAC, Zoom’s own privacy policy, promised consumers that “We do not allow third parties to use any personal data obtained from us for their own purposes, unless you consent.” ¶138. However, Zoom negligently failed to handle its users’ information with care, including a total lack of oversight in allowing users’ information to be collected by Facebook, failure to provide notice or obtain consent to share users’ information, and failure to vet or test third party software prior to implementation. ¶¶5-6, 10-11, 68, 73-105. As alleged, Zoom’s failure allowed Facebook to collect private data from Zoom users without permission or notice. *Id.* The information shared with Facebook is significant as it enables third parties to fingerprint individual devices and track users. *Id.* Zoom admitted its lack of care in providing Facebook access to Zoom users’ personal data, without the knowledge and consent of Zoom’s users. *Id.* at ¶13. These allegations are sufficient to establish a negligence claim. *See Facebook User Profile Litig.*, 402 F. Supp. 3d at 799 (allegations that Facebook failed to handle its users’ sensitive information with care were sufficient to plead a negligence claim).

b. Zoom Breached Its Duty to Warn

Zoom breached its duty to warn users of the risk of Zoombombing, including the risk that known offenders hijacked user meetings to show child pornography, hate speech, or other traumatizing images. *See e.g., Doe v. Internet Brands, Inc.*, 824 F.3d 846, 850 (9th Cir. 2016); *Putensen v. Clay Adams, Inc.* 12 Cal.App.3d 1062, 1076-1077 (1970) (the defendant has a “duty to use reasonable care to give warning of

⁷ Zoom does not argue that Plaintiffs failed to sufficiently plead the “duty” element of claims premised on Zoom’s failure to prevent third party data sharing, and therefore concedes that Zoom had a duty of care as described by Plaintiffs in the FAC. *See Kevin Barry Fine Art Assocs. v. Ken Gangbar Studio, Inc.*, 391 F. Supp. 3d 959, 969 n.3 (N.D. Cal. 2019) (Gilliam, J.) (finding waiver of arguments first raised in reply brief regarding whether allegations satisfied specific element of claim).

1 the dangerous condition of the product or of facts which make it likely to be dangerous to those whom he
 2 should expect to use the product or be endangered by its probable use, if the manufacturer has reason to
 3 believe that they will not realize its dangerous condition.)

4 Plaintiffs allege instances of Zoombombing that have occurred and continue to occur. ¶¶9, 37-38,
 5 41-42, 173-183. Nonetheless, Zoom did not warn its users that third parties, including known offenders,
 6 continued to hijack user video conferences. For example, Plaintiff Oak Life Church and its congregants
 7 were subjected to a Zoombombing incident whereby child pornography was displayed to church members.
 8 ¶¶41-42. The participants of the meeting were traumatized and devastated, and the Church was required
 9 to hire trauma counselors and establish support groups to assist the congregants. ¶41. Immediately
 10 following the April 19, 2020 incident, Oak Life Church reported the incident to Zoom, and in response,
 11 Zoom admitted that the intruder was a “**known offender**” and that the intruder had used the same IP
 12 address to attack Zoom’s network before. ¶42. Similarly, after Plaintiff Cundle reported a Zoombombing
 13 incident on May 6, 2020, Zoom admitted that the intruder was a “**known serial offender**” who had “been
 14 reported multiple times to the authorities.” ¶38. Thus, Zoom was negligent and failed to warn its users of
 15 the risk of Zoombombing and “known offenders” who were likely to attack certain users, including, and
 16 specifically, groups practicing their religion. A warning would not require Zoom to remove any user
 17 content or otherwise affect how users share content. Instead, Zoom could have warned users “perhaps by
 18 posting a notice on the website or informing users by email what it knew about the activities of” the known
 19 offenders. *See Internet Brands*, 824 F.3d at 851.

20 Zoom’s reliance on the “special relationship” requirement as articulated in *Tarasoff v. Regents of*
 21 *University of California* is misplaced. Mot. at 15, n. 11 (citing *Tarasoff v. Regents of Univ. of California*,
 22 17 Cal. 3d 425, 435 (1976)). That case concerned the special circumstances of a psychologist’s duty to
 23 warn a foreseeable victim about the dangerous proclivities of a patient. *Id.* The court observed there is
 24 no “duty to control the conduct of another” absent certain circumstances like a special relationship. *See*
 25 *id.* Notably, *Tarasoff* has been superseded by statute in California, and applies specifically to
 26 psychotherapists. Cal. Civ. Code § 43.92. Here, Plaintiffs’ cause of action is based on a long line of
 27 established precedent concerning failure to include adequate warning labels on products. *See e.g.*
 28 *Putensen*, 12 Cal.App.3d at 1076-1077. There is no “special relationship” requirement under a negligence

1 failure to warn product liability defect cause of action. *Id.*

2 **c. Plaintiffs Sufficiently Plead Damages for Negligence**

3 As explained above, Plaintiffs allege a variety of cognizable harms that they experienced as a
 4 direct and foreseeable result of Zoom’s conduct. As privacy is recognized as an inherent right, Zoom is
 5 charged by its duty of ordinary care to protect it. *Fairfield*, 138 Cal. App. 2d at 87–88; *Miller*, 187 Cal.
 6 App. 3d at 1481–82; *In re Facebook, Inc.*, 402 F. Supp. 3d at 802. Compensatory and nominal damages,
 7 in addition to any economic damages, are available to Plaintiffs whose privacy right was violated as a
 8 result of negligence or breach of contract. *See id.* at 802; *see also N. Am. Chem. Co. v. Superior Court*,
 9 59 Cal. App. 4th 764, 774, 69 Cal. Rptr. 2d 466, 470–71 (1997) (negligent failure to perform contract
 10 competently and reasonably “may be both a breach of contract and a tort. In such a hybrid circumstance,
 11 the plaintiff is entitled to pursue both legal theories until an occasion for an election of remedies arises.”).

12 Zoom’s arguments concerning organizational or associational standing are misplaced. First,
 13 organizational standing is an inherently fact-specific inquiry that cannot be determined on a motion to
 14 dismiss. *Planned Parenthood Fed’n of Am., Inc. v. Ctr. for Med. Progress*, 402 F. Supp. 3d 615, 705–06
 15 (N.D. Cal. 2019). Second, to the extent a showing of organizational standing is required at the pleading
 16 stage, Plaintiffs have amply done so by alleging damages and diversion of resources. *See Organic*
 17 *Consumers Ass’n v. Sanderson Farms, Inc.*, 284 F. Supp. 3d 1005, 1010 (N.D. Cal. 2018). The FAC
 18 provides, for example, that Plaintiff “Oak Life Church was required to hire trauma counsellors and
 19 establish support groups to assist its congregation in dealing with the resulting trauma.” ¶41. “At the
 20 pleading stage, a diversion-of-resources injury is sufficient to establish organizational standing even
 21 when it is ‘broadly alleged.’” *Organic Consumers Ass’n.*, 284 F. Supp. 3d at 1012.

22 In any event, the issue of damages is a fact-specific inquiry that is not appropriate for adjudication
 23 in a motion to dismiss. *See In re Facebook, Inc.*, 402 F. Supp. 3d at 799, n. 20.

24 **D. Plaintiffs State a Claim for Breach of Implied Contract**

25 “The existence of an implied contract is an issue of fact” inappropriate for determination on a
 26 motion to dismiss. *Castillo v. Seagate Tech., LLC*, No. 16-cv-01958-RS, 2016 WL 9280242, at *8 (N.D.
 27 Cal. Sept. 14, 2016). Plaintiffs plainly allege the formation of an implied contract, and Defendant does
 28 not dispute these allegations. ¶¶73-105, 106-110, 11-121, 124- 127, 102-105, 225-237.

1 “When a person hands over sensitive information . . . , they presumably expect to receive an
 2 implicit assurance that the information will be protected.” *Castillo*, 2016 WL 9280242, at *9. Courts
 3 have found such allegations sufficient. *See e.g., Hameed-Bolden v. Forever 21 Retail, Inc.*, 2018 WL
 4 6802818, at *3 (C.D. Cal. Oct. 1, 2018) (finding “implied contract” where “Defendants invited Plaintiffs
 5 and Class members to make purchases using their credit or debit cards” and thus agreed to “provide[]
 6 goods and services and . . . to safeguard and protect their Customer Data.”); *Gordon v. Chipotle Mexican*
 7 *Grill, Inc.*, 344 F. Supp. 3d 1231, 1247–48 (D. Colo. 2018) (“Plaintiffs state enough facts to plausibly
 8 allege the elements for an implied contract regarding the security of their PII that [Defendant] obtained in
 9 their transactions.”); *Rudolph v. Hudson’s Bay Co.*, No. 18-CV-8472 (PKC), 2019 WL 2023713, at *11
 10 (S.D.N.Y. May 7, 2019) (applying California law to uphold implied contract claim where “defendants
 11 promised to safeguard payment-card information in exchange for a customer’s payment”).

12 Zoom’s sole argument that any implied contract here is superseded by an express agreement should
 13 be rejected. Here, no express agreements were formed between the parties. ¶142. Thus, Zoom’s reliance
 14 on *Be In, Inc. v. Google Inc.*, No. 12-cv-03373, 2013 WL 5568706 (N.D. Cal. Oct. 9, 2013), is misplaced.
 15 *See Hickcox-Huffman v. US Airways, Inc.*, No. 10-cv-05193, 2017 WL 4842021, at *6 (N.D. Cal. Oct. 26,
 16 2017) (“In *Be In*, the court could dismiss the implied contract claim because both parties acknowledged
 17 the existence and substance of the express contract.”).

18 Zoom’s reliance on the mere existence of its Terms of Service (“TOS”) is insufficient to
 19 demonstrate that an express contract was formed between Plaintiffs and Zoom. Zoom has not submitted
 20 any evidence that Plaintiffs agreed to the TOS. Instead, Zoom submits a self-serving declaration that users
 21 cannot register for an account without clicking “confirm,” and that somewhere on that page the user is
 22 presented with the statement, “By signing up, I agree to the Privacy Policy and [TOS].” *See* Dkt. 121-1,
 23 Hill Decl. (hereinafter “Hill Decl.”) (attaching only the TOS and various iterations of the Privacy Policy
 24 itself). However, “where, as here, there is no evidence that the website user had actual knowledge of the
 25 agreement, the validity of the browsewrap agreement turns on whether the website puts a reasonably
 26 prudent user on inquiry notice of the terms of the contract.” *Nguyen v. Barnes & Noble Inc.*, 763 F.3d
 27 1171, 1177 (9th Cir. 2014); *see also Randall v. Change.org, Inc.*, 2020 U.S. Dist. LEXIS 231632, at *11
 28 n.5 (N.D. Cal. Dec. 9, 2020) (following *Nguyen* and finding that “pages were only hyperlinked to the

Solicitation and Contribution screens, making them ‘browsewrap agreements’ that are not enforceable as part of the contract absent evidence that the plaintiff had actual or constructive knowledge of their terms”); *Shultz v. TTAC Publ’g, LLC*, 2020 U.S. Dist. LEXIS 198834, at *9-*12 (N.D. Cal. Oct. 26, 2020) (same). Zoom does not indicate where the “I agree” statement appeared on the page in relation to the word “confirm,” how large the verbiage was, its color, or provide a screenshot of what Zoom users actually saw when signing up. What’s more, and importantly, Plaintiffs allege third parties like Facebook receive PII the second application installation begins, regardless of whether Plaintiffs created a Zoom account, and before Plaintiffs have even encountered the TOS. ¶85. Zoom’s declaration thus does not establish registrants had sufficient notice that they would be bound by the TOS. Indeed, this presents a disputed, triable issue of fact not appropriate for decision on a motion to dismiss. *Acri v. Varian Assocs., Inc.*, 121 F.3d 714 (9th Cir. 1997); *Pollstar v. Gigmania, Ltd.*, 170 F. Supp. 2d 974, 981-82 (E.D. Cal. 2000) (denying motion to dismiss where notice of browsewrap was an open question).

Even if the Court were to find the existence of an enforceable express contract, which there is not, the implied contract is based upon the exchange of benefits and PII, not on the matters contained in the TOS or Privacy Policy, and therefore does not concern the same subject matter or relevant scope. The only reference to PII in the TOS does not concern that exchange—rather, it states that “if Your Use of the Services requires Zoom to process any . . . PII . . . Zoom shall do so at all times in compliance with our Zoom Global Data Processing Addendum” Dkt. 121-1, Hill Decl., Ex. 1. The TOS simply does not govern Plaintiffs’ claims and the concern regarding artful pleading in *Dual Diagnosis Treatment Ctr., Inc. v. Blue Cross of Cal.*, SA CV 15-0736, 2016 WL 6892140, at *22 (C.D. Cal. Nov. 22, 2016), is not present here. The TOS provisions Zoom cites do not supersede the parties’ implied contract.

E. Plaintiffs Allege Breach of the Covenant of Good Faith and Fair Dealing

“Under California law, ‘[e]very contract imposes on each party a duty of good faith and fair dealing.’” *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-cv-2284-H-KSC, 2020 WL 2214152, at *6 (S.D. Cal. May 7, 2020) (quoting *Carson v. Mercury Ins. Co.*, 210 Cal. App. 4th 409, 429 (2012)). Plaintiffs allege Zoom failed to protect Plaintiffs’ and Class members’ PII, violated their privacy interests by disclosing PII without consent, disclosed such PII to unauthorized third parties for commercial purposes, and failed to timely notify Plaintiffs and Class members of the unlawful

disclosure, and that such failures were conscious and deliberate given that they contravened Zoom’s own policies. ¶¶73-87, 105-108, 124-125, 140-158, 240-243. Courts have found similar allegations sufficient. *See e.g., Solara*, 2020 WL 2214152, at *6; *In re Easysaver Rewards Litig.*, 737 F. Supp. 2d 1159, 1174 (S.D. Cal. 2010) (upholding claims that by sharing consumers’ financial account numbers the defendant “unfairly interfered with Plaintiffs and Class members’ rights to receive the security and privacy benefits they were entitled to under the contract”).

Courts also reject arguments that a claim for breach of the implied covenant of good faith and fair dealing is duplicative of a breach of contract claim where, as here, Plaintiffs allege that the Zoom “unfairly frustrated a benefit of the contract, that is, the confidentiality of the [plaintiff’s] financial information.” *Easysaver Rewards Litig.*, 737 F. Supp. 2d at 1174; *see also In re Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, *48 (N.D. Cal. Aug. 30, 2017) (“Although Defendants did not promise to employ ‘specific’ cybersecurity measures or ‘invest a particular sum of time or money’ in cybersecurity, Plaintiffs have sufficiently alleged . . . a contractual duty . . . for purposes of Plaintiffs’ claim under the implied covenant of good faith and fair dealing.”); *Davis v. Capitol Records, LLC*, No. 12-CV-1602 YGR, 2013 WL 1701746, at *4-5 (N.D. Cal. Apr. 18, 2013) (allegations of conduct depriving plaintiff of the benefits of the contract at issue are “sufficient to state a claim separate and distinct from her breach of contract claim.”).

While the breach of implied contract claim is based on Zoom’s failure to provide the services promised, the covenant claim is based on Zoom’s bad faith actions in disclosing its users’ PII without consent and misrepresenting its E2EE. ¶¶240-243. Such claims “will always be based on the same facts; a certain set of circumstances give rise to a lawsuit. They will always seek the same remedy; the same remedies are available for both claims. Therefore, the Court should not mechanically inquire whether the same facts are alleged and whether the same remedy is sought. Rather, the challenge . . . is to distinguish two claims based on the same facts.” *Celador Int’l Ltd. v. Walt Disney Co.*, 347 F. Supp. 2d 846, 852-53 (C.D. Cal. 2004) (finding claim “not superfluous”); *see also In re Premiera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2017 WL 539578, at *14 (D. Or. Feb. 9, 2017) (denying motion to dismiss implied contract claim arising from data breach under similar Oregon law). Plaintiffs’ allegations of Zoom’s bad faith conduct and improper use of users’ PII are sufficient. Finally, whether

Zoom's acted in bad faith is a question of fact that cannot be determined at the pleading stage.

F. Plaintiffs State Claims Under the UCL, CLRA, and for Fraudulent Concealment

1. Plaintiffs' Fraud-Based Claims Are Pled With Sufficient Particularity

Zoom overstates Plaintiffs' burden under Rule 9(b). To satisfy Rule 9(b)'s heightened pleading standard, "the allegations must be '*specific enough to give defendant[] notice of the particular misconduct which is alleged* . . . so that they can defend against the charge and not just deny that they have done anything wrong.'" *Davidson v. Apple, Inc.*, No. 16-cv-4942-LHK, 2017 WL 976048, at *4 (N.D. Cal. Mar. 14, 2017) (quoting *Semegen v. Weidner*, 780 F.2d 727, 731 (9th Cir. 1985) (emphasis added)). Plaintiffs allegations detail Zoom's misleading statements and key omissions, all of which obscured Zoom's subpar security capabilities and practice of sharing specific user information with third parties. See ¶¶74, 77-86, 107-10, 124-26, 129-43, 163-68, 181.

Zoom seeks dismissal under Rule 9(b) but, as discussed further below, Rule 9(b) does not apply to the extent that liability for these claims—including claims under California's Unfair Competition Law—are based on non-fraudulent conduct. See *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1104 (9th Cir. 2003) ("[Rule 9(b)] does not require that allegations supporting a claim be stated with particularity when those allegations describe non-fraudulent conduct.").

2. Plaintiffs Sufficiently Allege Claims Based On Affirmative Statements

Plaintiffs advance claims based on affirmative statements by Zoom which were likely to deceive consumers. With respect to this liability theory, "Rule 9(b) does not demand that plaintiffs research and present a detailed exposé in their complaint." *Brickman v. Fitbit, Inc.*, No. 15-cv-2077-JD, 2016 WL 3844327, at *2 (N.D. Cal. July 15, 2016). Instead, Rule 9(b) can be satisfied simply by identifying the statements on Zoom's website and privacy policy that are reasonably likely to mislead. See *id.* The FAC therefore does not need to "expressly allege when and where Plaintiff[s] saw the statements." *Ehret v. Uber Technologies, Inc.*, 68 F. Supp. 3d 1121, 1129 (N.D. Cal. 2014). Requiring more, "would be unrealistic and needlessly impede access to [] important remedial . . . statute[s]." *Id.*

Plaintiffs allege several affirmative statements by Zoom regarding its management of customer data and its security features including E2EE. ¶¶129-39, 163-66. Moreover, by alleging that Zoom's statements regarding privacy and security did not disclose relevant information regarding data-sharing with third parties and actual security capabilities, "Plaintiffs adequately allege the 'who what when and

how,’ given the inherent limitations of an omission claim.” *Philips v. Ford Motor Co.*, No. 14-cv-2989-LHK, 2015 WL 4111448, at *12 (N.D. Cal. July 7, 2015) (quoting *MacDonald v. Ford Motor Co.*, 37 F. Supp. 3d 1087, 1096 (N.D. Cal. 2014) (“an omission-based fraud will not be able to specify the time, place, and specific content of an omission as would a plaintiff in a false representation claim”) (internal quotations omitted)). ¶¶74, 77-86, 107-10, 124-26, 129-43, 163-68, 170-71, 181. These allegations satisfy Rule 9(b).

3. Plaintiffs Adequately Allege Reliance

Zoom’s argument that Plaintiffs failed adequately to allege reliance misstates the legal standard and ignores well-pleaded facts. *See Gitson v. Trader Joe’s Co.*, No. 13-cv-1333-WHO, 2014 WL 1048640, at *8 (N.D. Cal. Mar. 14, 2014) (explaining that plaintiffs can allege reliance “by alleging that [they] would not have bought the product but for the alleged misrepresentation”); *Shin v. BMW of N. Am.*, No. CV 09-398-AHM, 2009 WL 2163509, at *4 (C.D. Cal. July 16, 2009) (“Plaintiffs are not required to plead ‘reliance’ . . . with particularity”). The FAC includes numerous well-pleaded allegations that Plaintiffs relied on Zoom’s misrepresentations and/or would not have purchased Zoom but for the alleged misrepresentations. ¶¶18-19, 22-23, 26, 28, 30, 34-35, 40, 44, 47-48, 51-52, 54, 57, 59. These specific allegations do not contradict the more general allegation that many people are required to use Zoom in order to access services during the pandemic. *Cf. In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1231 (N.D. Cal. 2014) (“Accordingly, the Court finds that Plaintiffs have not pleaded themselves out of court by alleging that they did not cancel their Creative Cloud subscriptions upon learning of Adobe’s omissions regarding security.”).

4. Plaintiffs Adequately Allege Fraud-Based Claims

Zoom’s argument that Plaintiffs must plead additional facts regarding how Zoom’s promises were false *as to them* finds no support in the law. Zoom argues that Plaintiffs failed to allege which third-party apps or services collected *their* personal information. As explained above, Plaintiffs’ allegations are “specific enough to give defendant[] notice of the particular misconduct which is alleged,” including the “specific content of the false representations.” *Davidson*, 2017 WL 976048, at *4, *7 (citations omitted).

Zoom’s argument relies upon a strained reading of *Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840, 850 (N.D. Cal. 2012). Applying Rule 9(b), *Pirozzi* concluded that plaintiff failed to allege which statements

made by Apple she was exposed to or relied upon in her decision to purchase Apple products or apps. However, *Pirozzi* does not require that Plaintiffs plead how misleading statements *were false as to them*.

5. Plaintiffs State a CLRA Damages Claim

Zoom concedes that Plaintiffs Hartmann, Hirshberg, Garcia, and Doyle are consumers under the CLRA.⁸ It requests dismissal with prejudice of their claims for damages for failure to provide pre-suit notice, despite the fact that Plaintiffs' counsel served Zoom with a CLRA notice and Zoom refused to rectify the violations. ¶276, 278. Accordingly, dismissal would be unwarranted and draconian in light of the purpose of the notice requirement. This requirement is designed to provide defendants an opportunity to avoid liability by correcting the alleged wrong. *Morgan v. AT & T Wireless Servs., Inc.*, 177 Cal. App. 4th 1235, 1261 (2009). Thus, wholesale dismissal with prejudice does not follow—instead, courts dismiss CLRA damages claims without prejudice until after the notice requirement is satisfied. *Id.* Following this logic, federal courts conclude that failure to provide pre-suit notice is not a reason to dismiss a CLRA claim for damages *with prejudice*. See *Elias v. Hewlett-Packard Co.*, 903 F. Supp. 2d 843, 857 n.4 (N.D. Cal. 2012) (“Plaintiff is not prevented from amending the complaint to include a request for CLRA damages”) (citing *Morgan*, 177 Cal. App. 4th at 1261); see also *Oxina v. Lands' End, Inc.*, No. 14-cv-2577-MMA, 2015 WL 4272058, at *3 (S.D. Cal. June 19, 2015) (rejecting cases Zoom relies on and collecting cases following *Morgan*). Thus, if the Court determines that dismissing Plaintiffs' CLRA damages claim is required, it should do so without prejudice so that Plaintiffs may provide notice.

6. All Plaintiffs Suffered Economic Injury

Zoom concedes that several Plaintiffs sufficiently allege economic injury for standing under the UCL. Its argument that only Plaintiffs who paid Zoom can maintain a UCL claim misconstrues the UCL's statutory standing requirement. For statutory standing, the UCL requires only economic injury and causation, which Plaintiffs allege. *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016) (citing *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310 (2011)). In addition to allegations that defendant wrongfully possesses plaintiff's money—which Zoom suggests are required—economic injury also encompasses, for example, having overpaid a third party due to the unfair conduct. See *Kwikset*, 51 Cal. 4th at 323-25 (collecting cases); *Aron v. U-Haul Co.*, 143 Cal. App. 4th 796, 802-03 (2006) (economic

⁸ Zoom's argument that Plaintiff Gormezano admits to using Zoom's services for free also fails because Plaintiff Gormezano alleged paying for a Zoom Pro Account. ¶ 50.

injury for UCL alleged where plaintiff overfilled a fuel tank to avoid defendant’s fuel charge); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 840 (N.D. Cal. 2020) (“To be clear, the Court is not requiring Plaintiffs to show they are entitled to restitution under the UCL in order to establish their standing under the UCL.”).

Here, Plaintiffs—including those who didn’t directly pay Zoom—properly allege they suffered economic injury. For example, Plaintiff Gmerek used Zoom for sessions with her psychologist, which she expected to be private. Lacking privacy safeguards diminished the value of the medical care for which she paid. ¶23; see *In re Vizio Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1217 (C.D. Cal. 2017) (undisclosed privacy-related deficiencies in paid-for products and services constitute economic injury). In fact, the devaluation of many paid-for services conducted over Zoom is a cornerstone of the FAC. See ¶¶171 (no doctor-patient interactions on Zoom were truly private), ¶¶173-83 (businesses and their consumers alike were damaged by incidents of “zoombombing”).

7. Plaintiffs State Claims Under The UCL’s Unlawful and Unfair Prongs

The “unlawful” prong of the UCL requires only that a business practice be “forbidden by law.” *In re Adobe Sys.*, 66 F. Supp. 3d at 1225 (quoting *Cel-Tech Commc’ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999)). As described in detail above, Zoom’s practices satisfy this requirement.

Zoom’s contention that each Plaintiff must march through each element of each predicate legal violation overstates the pleading requirements for the UCL’s unlawful prong. *Compare* Mot. at 24 & n.15 (arguing for dismissal because Plaintiffs “do not indicate how any particular Plaintiff’s experience with Zoom meets the requirements for a COPPA violation”), with *In re Anthem*, 162 F. Supp. 3d at 989 (no such requirement). Plaintiffs identify legal violations beyond the causes of action with sufficient detail, and the FAC’s allegations support those violations. See ¶¶171, 184-189, 255.

Zoom is also incorrect that the FAC’s allegations are “conclusory” with respect to the UCL’s unfair prong—it is replete with allegations of unfairness and injury to users. *Compare* Mot. at 25 (citing only one paragraph of the FAC under the UCL Cause of Action heading), with, e.g., *Sagana v. Tenorio*, 384 F.3d 731, 736 (9th Cir. 2004) (plaintiffs must provide “fair notice” of a claim and its basis without regard for technical formalism). Specifically, Plaintiffs allege that Zoom knowingly maintains lax data security “on par with some of the worst of today’s tech giants” in a time when it is most important ¶¶12-15, 72;

Zoom shares extensive user data with Facebook, Google, and others, without consent or even notification ¶¶73-128; and that Zoom promises privacy and security while exposing their private information to unauthorized parties, failing to provide industry-standard security, and putting them at risk of emotional harm from Zoombombers. ¶¶129-37, 159-83.

G. Plaintiffs State a Claim for Unjust Enrichment

A claim for unjust enrichment can proceed as an independent cause of action. A court may construe a cause of action as a quasi-contract claim seeking restitution. *See Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015); *Swafford v. IBM*, 383 F. Supp. 3d 916, 931 (N.D. Cal. 2019). Unjust enrichment and restitution “describe the theory underlying a claim that a defendant has been unjustly conferred a benefit through mistake, fraud, coercion, or request,” or a situation where “restitution require[s] a party to return a benefit when the retention of such benefit would unjustly enrich the recipient.” *Astiana*, 783 F.3d at 762 (quotation marks and citations omitted); *see also Facebook Internet Tracking*, 956 F.3d at 599 (“California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss.”).

Contrary to Zoom’s assertion, dismissal would be inappropriate even if the Court were to conclude the unjust enrichment claim is duplicative of the CLRA or UCL claims. *Astiana*, 783 F.3d at 762 citing Fed. R. Civ. P. 8(d)(2) (“A party may set out two or more statements of a claim or defense alternatively or hypothetically, either in a single count or defense or in separate ones.”); *see also Bruton v. Gerber Prods. Co.*, No. 12-CV-02412-LHK, 2018 U.S. Dist. LEXIS 149404, at *25 (N.D. Cal. Aug. 31, 2018) (rejecting argument that unjust enrichment claim should be dismissed because it was duplicative of UCL claim); *Clear Channel Outdoor, Inc. v. Bently Holdings Cal. L.P.*, No. 11-2573 EMC, 2011 WL 6099394, at *9 (N.D. Cal. Dec. 7, 2011) (“[E]ven though a plaintiff may not ultimately prevail under both unjust enrichment and breach of contract, it may plead both in the alternative.”). And finally, Zoom’s argument that a claim for unjust enrichment fails because the parties previously entered into a contract fails for the same reasons described in section III.D. above.

H. Plaintiffs’ CDAFA Claim Should Not Be Dismissed

The Ninth Circuit recently reversed dismissal of a CDAFA claim under analogous circumstances in a controlling opinion omitted by Zoom. *Facebook Internet Tracking* held plaintiffs sufficiently alleged

injury for purposes of their CDAFA claim because they “adequately pleaded an entitlement to Facebook’s profits from users’ personal data” under California law, and that the data at issue—their browsing histories—“carry financial value.” 956 F.3d at 600. Plaintiffs also allege that the data Zoom shared with third parties is valuable, and that Plaintiffs are entitled to Zoom’s profits resulting from its unauthorized sharing. ¶¶112, 244-49. *Facebook Internet Tracking* dispenses with Zoom’s argument that Plaintiffs somehow fail to allege the requisite “‘damage or loss.’” Mot. at 19 (quoting Cal. Penal Code § 502(e)(1)). Under *Facebook Internet Tracking*, Zoom’s citation to cases such as *In re Apple & ATTM Antitrust Litig.*, No. C 07-05152, 2010 WL 3521965 (N.D. Cal. July 8, 2010) (cited in Mot. at 20), is inapposite in that they were wrong to hold plaintiffs lacked standing.

Plaintiffs allege Zoom transferred their PII to Facebook and other third parties without any permission whatsoever. Accordingly, it is not simply “the method” by which Zoom accessed the information that is alleged to violate CDAFA, but the entirety of Zoom’s practice of transferring such data, and authority such as *Brodsky v. Apple Inc.*, No. 19-CV-00712, 2019 WL 4141936, at *9 (N.D. Cal. Aug. 30, 2019), and *Ticketmaster LLC v. Prestige Entm’t W., Inc.*, 315 F. Supp. 3d 1147, 1175 (C.D. Cal. 2018), that do not support Zoom’s position.

Finally, far from constituting a simple recitation of CDAFA’s statutory requirements, the FAC alleges in detail how Zoom violated Cal. Penal Code § 502(c)(1), (2), (3), and (7) by accessing and taking, without permission, Plaintiffs’ and Class members’ PII including “device and location data” (¶¶282-83); “violated §§ 502(c)(6) and (c)(13) . . . by knowingly and without permission . . . providing third parties[] including . . . a means of accessing Plaintiffs’ and Class members’ computers and mobile devices” (¶285); and violated § 502(c)(8) by introducing a “computer contaminant” that allowed the exfiltration (¶¶286-87). Although Plaintiffs voluntarily used Zoom, they did not voluntarily agree to collection and use of their PII. Accordingly, Plaintiffs adequately allege that Zoom acted “‘without permission.’” Mot. at 19 (quoting Cal. Penal Code § 502(c)(1)-(3), (6)-(7), and (13)).

IV. CONCLUSION

Plaintiffs respectfully request that the Court deny Zoom’s motion to dismiss in its entirety. To the extent the Court grants any portion of the motion to dismiss, Plaintiffs request leave to amend. Fed. R. Civ. P. 15.

Respectfully submitted,

Dated: December 30, 2020

/s/ Tina Wolfson

Tina Wolfson
twolfson@ahdootwolfson.com
AHDoot & WOLFSON, PC
2600 West Olive Ave., Suite 500
Burbank, CA 91505
Tel: (310) 474-9111
Fax: (310) 474-8585

/s/ Mark C. Molumphy

Mark C. Molumphy
mmolumphy@cpmlegal.com
COTCHETT, PITRE & MCCARTHY, LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Tel: (650) 697-6000
Fax: (650) 697-0577

Interim Co-Lead Counsel for Plaintiffs

Rachele R. Byrd
byrd@whafh.com
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
Symphony Towers
750 B Street, Suite 1820
San Diego, CA 92101
Tel: (619) 239-4599
Fax: (619) 234-4599

Albert Y. Chang
achang@bottinilaw.com
BOTTINI & BOTTINI, INC.
7817 Ivanhoe Avenue, Suite 102
La Jolla, CA 92037
Tel: (858) 914-2001
Fax: (858) 914-2002

Eric H. Gibbs
ehg@classlawgroup.com
GIBBS LAW GROUP LLP
505 14th Street, Suite 1110
Oakland, California 94612
Tel: (510) 350-9700
Fax: (510) 350-9701

Plaintiffs' Steering Committee

ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)

I, Mark C. Molumphy, attest that concurrence in the filing of this document has been obtained from the other signatory. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 30th day of December 2020, at Burlingame, California.

/s/ Mark C. Molumphy

Mark C. Molumphy